Customer No. 24498
Attorney Docket No. PU030241
Final Office Action Date: 11/08/10

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicants: ZHANG, Junbiao, et al.	Examiner: VU, Phy Anh Tran
Serial No: 10/567, 271	Group Art Unit: 2437
Filed: February 6, 2006	Docket: PU030241

For: METHOD AND DEVICE FOR SECURING CONTENT DELIVERY OVER A COMMUNICATION NETWORK VIA CONTENT KEYS

Mail Stop Appeal Brief-Patents
Hon. Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Applicants appeal the status of Claims 1–31 as rejected in the final Office Action dated November 8, 2010, pursuant to the Notice of Appeal filed March 7, 2011 and submit this appeal brief. Please charge the fee for the Brief, the fee for extending the deadline for filing the Brief, and any other fees in connection with this filing to Deposit Account 07-0832.

TABLE OF CONTENTS:

1. Real Party in Interest

The real party in interest is THOMSON LICENSING, the assignee of the entire right title and interest in and to the subject application by virtue of two assignments recorded with the Patent Office on February 6, 2006 at reel/frame 017545/0830 and at reel/frame 017545/0894.

2. Related Appeals and Interferences

Appellant is not aware of any appeals or interferences related to the present application.

3. Status of Claims

Claims 1–31 are pending. Claims 1, 10 and 16 are independent. Claims 1–31 stand rejected and are under appeal.

A copy of the Claims 1–31 is presented in Section 8 below.

4. Status of Amendments

A response to a non-final Office Action, dated May 6, 2010, was filed and entered on August 19, 2010. No responses/amendments were filed subsequent to the August 19, 2010 response. The claims listed in section 8 "Claims Appendix" of this Appeal Brief correspond to the claims submitted in Appellant's response on August 19, 2010.

5. Summary of Claimed Subject Matter[1]

The invention generally relates to an arrangement for transferring content between a content server (CS) and a content consumer (CC), in a network environment, wherein a content requester (CR) initiates the request to download the content between the content server and the content consumer. It may be desirable for a CR to request that content be downloaded to a separate CC from a CS, for example, when the CR is operating in a low bandwidth environment, wherein it is more efficient to download the content to a device other than the CR (see, paragraph 0004). In particular, the invention provides a system for enabling the CS to receive a request from the CR, and then verify the CC before transmitting the content to the CC.

The claimed invention, as recited in claim 1, is directed to a device, located at a remote site in communication with a network having at least one server and a content requester, comprising: - a processor in communication with a memory (page 9, paragraph [00034] and Fig. 7), said processor operable to execute code for: receiving a first information item comprising an access code and a content key scrambled using a key known by said device(page 4, paragraph [00018] and Fig. 2), said access code generated by said at least one server in response to a request for a second information item provided by the content requester (page 4, paragraph [00018] and Fig. 2); descrambling said first information item using the key known by said device (page 5, paragraph

[1] *It should be explicitly noted that it is not the Appellant's intention that the currently claimed or described embodiments be limited to operation within the illustrative embodiments described below beyond what is required by the claim language. Further description of the illustrative embodiments are provided indicating portions of the claims which cover the illustrative embodiments merely for compliance with requirements of this appeal without intending to read any further interpreted limitations into the claims as presented.*

[00019] and Fig. 2); transmitting said access code to a server hosting said second information item (page 5, paragraph [00019] and Fig. 2); and receiving said second information item scrambled using said content key after said server hosting the second information item verifies said access code (page 5, paragraph [00019] and Fig. 2).

The claimed invention, as recited in claim 10, is directed to a method, operable at a receiving device located at a remote site in communication with a network having at least one server and a content requester, for descrambling secure content received over said network, said method comprising the steps of: receiving a first information item comprising an access code and a content key scrambled using a key known by said receiving device(page 4, paragraph [00018] and Fig. 2), said access code generated by said at least one server in response to a request for a second information item by the content requester (page 4, paragraph [00018] and Fig. 2); descrambling said first information item using the key known by said receiving device (page 5, paragraph [00019] and Fig. 2); transmitting said access code to a server hosting said second information (page 5, paragraph [00019] and Fig. 2); receiving said second information item, scrambled using said content key, after said server hosting the second information item verifies said access code (page 5, paragraph [00019] and Fig. 2); and descrambling said second information item using said content key(page 5, paragraph [00019] and Fig. 2).

The claimed invention, as recited in claim 16, is directed to a method for transferring secure content over a network comprising the steps of: receiving a request for content at a first server over a first network from a file requesting device, said request including an encryption key known to a designated remote site (pages 3-4, paragraph

[00016] and Fig. 2); generating a first information containing an access code and a content key at said first server in response to said request for content by said file requesting device (page 4, paragraph [00018] and Fig. 2); transferring said first information item to said designated remote site having a file receiving device, wherein said access code and said content key are scrambled using said encryption key (page 4, paragraph [00018] and Fig. 2); receiving said access code from said designated remote site having said file receiving device (page 4, paragraph [00018] and Fig. 2); and transferring secure content over a second network after verification of said access code, wherein said secure content is encrypted using said content key (page 5, paragraph [00019] and Fig. 2).

6. Grounds of Rejection to be Reviewed on Appeal

Claims 1–2, 4-5, 10-13, and 29-30 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,385, 317 to Rix et al (hereinafter "Rix") and further in view of US Patent Application No. 2002/0032665 to Creighton et al (hereinafter "Creighton").

Claims 16–20, 23-27, and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix and further in view of US Patent No. 7,392,393 to Taki (hereinafter "Taki").

Claims 3 and 6 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Creighton, and further in view of US Patent Application No. 2004/0049464 to Ohmori (hereinafter "Ohmori").

Claims 7-9 and 14-15 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Creighton, and further in view of WO 02/32026 issued to Henrick (hereinafter "Henrick").

Claims 21 and 28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Taki, and Henrick.

Claim 22 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Taki, and further in view of US Patent Application No. 2001/0056404 to Kuriya et al (hereinafter "Kuriya").

The preceding rejections under 35 U.S.C. § 103(a) are presented for review in this Appeal with respect to Claims 1–31, as argued with respect to independent Claims 1, 10, and 16.

Regarding the grouping of the claims with respect to the rejections under 35

U.S.C. §103(a), Claims 1 – 9 and 29 stand or fall with Claim 1 due to their respective dependencies therefrom. Claims 10 – 15 and 30 stand or fall with claim 10 due to their respective dependencies therefrom. Claims 16 – 28 and 31 stand or fall with claim 16 due to their respective dependencies therefrom.

7. Argument

A. CLAIMS 1–2, 4-5, 10-13, AND 29-30 ARE PATENTABLY DISTINGUISHABLE UNDER 35 U.S.C. § 103(A) OVER RIX AND FURTHER IN VIEW OF CREIGHTON.

The failure of an asserted combination to teach or suggest each and every feature of a claim remains fatal to an obviousness rejection under 35 U.S.C. § 103. Section 2143.03 of the MPEP requires the "consideration" of every claim feature in an obviousness determination. To render a claim unpatentable, however, the Office must do more than merely "consider" each and every feature for this claim. Instead, the asserted combination of the patents must also teach or suggest each and every claim feature. *See In re Royka*, 490 F.2d 981 (CCPA 1974) (emphasis added) (to establish prima facie obviousness of a claimed invention, all the claim features must be taught or suggested by the prior art).

Applicants respectfully submit that Claims 1–2, 4-5, 10-13, and 29-30 are patentable over Rix and further in view of Creighton because the references, singly and in combination, fail to teach or suggest each and every limitation of Claims 1–2, 4-5, 10–13, and 29–30.

1. Rix does not recite, disclose or suggest "receiving a first information item comprising an access code and a content key scrambled using a key known by said device, said access code generated by said at least one server in response to a request for a second information item provided by the content requester" as recited in claim 1.

Rix relates to a system for providing secure communications between devices in a pay TV environment, in particular between a control access module ("CAM") and a smart card, coupled to each other through a dedicated connection slot, or a decoder and a conditional access module, in order to prevent unauthorized operation of a decoder (col. 1, lines 21-25).

Specifically, Rix seeks to prevent the use of an unauthorized smart card in combination with a CAM (col. 2, lines 47-50). When the smart card is inserted into the CAM, the CAM generates a random key C_i that is used to encrypt and decrypt communications between the smart card and the CAM (col. 1, lines 26 – 40). The CAM also generates a random number *A*. The CAM encrypts the random key C_i and *A* using the CAM's public key and transmits them to the smart card (col. 2, lines 54 – 56). The smart card decrypts the message using the CAM's private key (col. 2, lines 56 – 59) and transmits the number *A* to the CAM encrypted with C_i (col. 2, lines 59 – 62). When the CAM receives back the number *A*, it knows that the smart card is authorized (col. 2, lines 64 – 67). Once the smart card is authorized, the CAM sends ECMs containing the encrypted control word to the smart card. The ECMs contain a control word that is encrypted using a service key. The service key is downloaded to the smart card through an entitlement management message (col. 2, lines 36 – 38). From then on, communications between the smart card and the CAM will carry the control word encrypted with the key C_i (col. 3, lines 4-7).

Applicants submit that Rix fails to teach or suggest the feature of a device in communication with a network having at least one server and the content requester as recited in claim 1.

The Examiner apparently interprets the recited "server" to correspond to the CAM of Rix asserting that the CAM provides services for other devices, and the recited "network" to correspond to the connection slot on the CAM, which only the smart card can plug into. See, Final Office Action dated November 8, 2010, on page 2 in Response to Arguments, "First of all, a server is broadly defined as any device that provides services for other devices. Secondly, a network is defined as two or more devices interconnected by communications channels that facilitate communications."

The Examiner's construction of the CAM of Rix as the server of the claimed invention, and the connection between the CAM with a smart card via a connection slot of the decoder as a network of the claimed invention, is not an interpretation considered by Applicants' specification and is not an interpretation that one of ordinary skill in the art would make in view of the specification.

MPEP 2111 states that "[t]he Patent and Trademark Office ("PTO") determines the scope of claims in patent application not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction ***"in light of the specification as it would be interpreted by one of ordinary skill in the art.*** " *In re Am. Acad. Of Sci. Tech. Ctr.*, 367 F. 3d 1359, 1354 [70 USPQ2d 1827] (Fed. Cir. 2004) (emphasis added).

Applicants' specification makes reference to the content server being in communication through a network. The network is described as a "low speed wireless network" (paragraph [00015]), a "high-speed network, such as the Internet or a specialized content delivery network (CDN)" (paragraph [00015]), "a local area network connected to the Internet" (paragraph [00015]) One of ordinary skill in the art would not read Applicants' specification and interpret the term "server" to be a conditional access module that has no capability to communicate with any network, including the Internet. Rather, the CAM of Rix communicates with the smart card through a connection slot.

Nor would one of ordinary skill in the art read Applicants' specification and interpret the term "network" to be a connection slot, which provides a connection between only the smart card and the CAM. Rix, at paragraph 2, lines 11 – 13 states that "the decoder further comprises a conditional access module or CAM 4 and a smart card 5 which can be inserted into a connection slot of the conditional access module 4." The CAM and the smart card communicate through the connection slot on the CAM which the Examiner interprets as corresponding to a network. The connection slot in Rix is specifically tailored for smart cards that are paired with the CAM. Only one smart card can connect into the connection slot of Rix at any point in time. One of ordinary skill in the art would not interpret a network to be a connection slot that has no capability to communicate with the Internet and which can only communicate with a paired smart card.

Furthermore, the Examiner in the Final Office Action dated November 8, 2010 ("Final Office Action") on pages 2 – 3 contends that the "request for a second information item provided by the content requester" of claim 1 is taught in Rix by the insertion of a smartcard into a conditional access module ("CAM") by a subscriber. (See Final Office Action page 2, "By inserting the smartcard into the CAM, the subscriber is indirectly requesting to receive a control word, so that the control word can be used to descramble digital data stream of the subscribed program." See page 3, "So, in response to the subscriber inserting the smartcard into the CAM to request for the control word, the CAM generates two random numbers…").

However, the subscriber of Rix is a **user** of a pay TV system, not a **device** in communication with a network. Claim 1 recites that the content requester is part of a network and the specification clearly indicates that the content requester is an electronic device (see Specification, paragraph [00015]). Since the subscriber of Rix is not an electronic device in communications with a network, the insertion of the smart card into the CAM cannot correspond to a request for a second information item provided by the content requester as recited in claim 1.

The Examiner in page 3 of the Final Office Action contends that

"said access code generated by at least one server in response to a request for a second information item provided by the content requester" of claim 1 is taught in Rix when "the CAM generates two random number Ci (content key) and A (access code) (corresponding to the recited said access code generated by said at least one server in response to a request for a second information item provided by the content requester) (Column 2, lines 52-54)."

In other words, the Examiner is contending that the conditional access module of Rix is a server. However, for the reasons discussed above, Applicants respectfully submit that the conditional access module of Rix does not correspond to the recited server, and Rix fails to teach or suggest the device being in communications with a network having at least one server and a content requester as recited in claim 1.

Accordingly, Rix does not teach or suggest that the "access code was generated by at least one server in response to a request for a second information item provided by the content requester."

2. Rix does not teach or suggest "transmitting said access code to a server hosting said second information item" as recited in claim 1.

The Examiner contends in the Final Office Action on page 3 that

"[u]pon receiving the encrypted generated random numbers Ci and A, the smartcard, decrypted it, and send back to the CAM the random number A encrypted with random Ci (corresponds to transmitting said access code to a server hosting said second information item) (Column 2, lines 59-62)."

Again, the Examiner is construing the CAM as a "server hosting said second information item." As noted above, one skilled in the art would not interpret a CAM as a server.

The Examiner's interpretation that the CAM may be considered a server and the second information item is the control word is not consistent with the teachings of Rix. Under the Examiner's interpretation, the CAM would be hosting the control word. Rix discloses that the control word is transmitted via an entitlement control message (page 2, lines 39 – 42). One of ordinary skill in the art would recognize that in this arrangement the CAM is merely a decoder and that the control words transmitted in entitlement control messages are hosted by a satellite or cable service provider, and not by the CAM. Accordingly, the Examiner's interpretation of the term "server" is not a reasonable construction in light of Applicants' specification and would not be interpreted as such by one of ordinary skill in the art. As such, Rix does not teach or suggest "transmitting said access code to a server hosting said second information item."

3. Rix does not teach or suggest "receiving said second information item scrambled using said content key after said server hosting the second information item verifies said access code."

In the Final Office Action on page 3, the Examiner contends that

"once the random number A (access code) is verified, the CAM forward the entitlement control message which contains the encrypted control word to the smartcard. It is interpreted by the Examiner that the encrypted control word is indirectly encrypted with the random number Ci, because after the random number A has been verified, key Ci (content key) is used in all communications between the smartcard and the CAM."

The Examiner cites page 6, column 2, line 62 through column 3, lines 7 as support in Rix for this interpretation.

The Examiner misapplies the notion of receiving the entitlement control message containing the control word with a return message that is sent from the smart card to the CAM containing the control word encrypted with Ci.

Rix at paragraph 2, lines 33 – 38 states:

"[i]n a pay TV system the control word required for descrambling, is transferred to the subscribers in so-called entitlement control messages containing the control word **encrypted using a service key.** This service key is downloaded in the memory 11 of the smart card 5 by means of a so-called entitlement management message for example" (emphasis added).

This section clearly indicates that the entitlement control message containing the control word is encrypted using a service key and not the content key as contended by the Examiner.

By contrast, claim 1 recites "receiving said second information item scrambled using said **content key** after said server hosting the second information item verifies said access code" (emphasis added). The content key of claim 1 does not correspond to the service key of Rix. Accordingly, the element "receiving said second information item scrambled using said content key after said server hosting the second information item verifies said access code" is not taught or suggested in Rix.

Creighton is cited by the Examiner as disclosing the feature of "said access code is transmitted to different server other than the at least one server." Irrespective of Creighton's teaching in that regard, Appellants submit that Creighton does not in any way cure the deficiencies present in Rix as discussed above for claim 1, as there is no showing of Creighton teaching or suggesting the above claimed features missing in Rix.

4. <u>There is no motivation to combine Rix and Creighton</u>

The Examiner provides a very generic motivation for combining Rix and Creighton, stating in the Final Office Action on page 4:

"both Rix and Creighton disclose the concept of providing resources to device that has been authenticated. In Rix, the CAM performs both authenticating, and providing content, once the device has been authenticated. Creighton discloses a system that delegates different tasks to different entities, each of which is more effectively and efficiently specialized in solving a particular task. **As such, both Rix and Creighton are about authenticating access requests.** Therefore, one of ordinary skill in the art would have been motivated to incorporate the teachings of Creighton into the method and/or system taught by Rix to achieve the advantage as described in the Office Action" (emphasis added).

In addition, on page 6 of the Final Office Action, the Examiner contends that

"[o]ne of ordinary skill in the art at the time the invention was made would have been motivated to incorporate the structure of Creighton into the device of Rix to provide for an effective and efficient system of distributing tasks ([0007]).

The Examiner cites paragraph [0007] of Creighton as a rationale for the motivation to combine Creighton and Rix. Paragraph [0007] of Creighton states the following:

> When there are a few authorized parties, the equipment manufacturer can authenticate and authorize each one of the parties. However, when the number of authorized parties becomes large, the equipment manufacturer maybe forced to have a staff dedicated for the purpose of authenticating and authorizing each party requesting access to its proprietary information. This is a situation that the equipment manufacturer may not like to occur, since the equipment manufacturer is not in the market place to authenticate and to authorize third parties.

Applicants submit that the generic motivation cited by the Examiner does not provide sufficient basis to establish that a person of ordinary skill in the art would have combined disparate teachings in the different cited references as required by the claims. Each reference solves an entirely different problem and the combination does not produce the claimed invention.

Rix is concerned with the secure communication between a smart card and a CAM in order to prevent the switching of an authorized smart card with an unauthorized smart card (Rix, col. 1, lines 16 – 20). Creighton is concerned with authorizing business partners to access information from a central website accessible via the Internet with the use of digital certificates (Creighton, paragraph [0002] and [0010]). These are entirely different environments having different considerations and problems.

By contrast, the claimed invention is concerned with allowing a content requester to send a request to a content server to download content to a device. The claimed invention ensures that both the content requester is authorized to make the request for the content and that the device is authorized to receive the content. In addition, the claimed invention ensures that the content is securely transmitted to an authorized device.

Neither Rix nor Creighton address or solve this specific problem. In fact, as noted above, the Examiner has admitted that "both Rix and Creighton are about authenticating access requests." However, the Examiner ignores the fact that the claimed invention is directed to more than merely authenticating an access request. The claimed invention is in the context of a specific arrangement and seeks to ensure that a device is authorized to receive content and to ensure that the content is securely transmitted to an authorized device.

Furthermore, one skilled in the art would not be motivated to combine Rix and Creighton because they involve entirely different environments and address entirely different problems. The structure of Creighton relies on business parties communicating through online transactions communicated over a network. Rix pertains to secure communications between a smart card that is inserted into a CAM. The smart card and the CAM are not in communication with a network. As such, Rix is not suited or structured to operate in a network environment. Similarly, the solution of Creighton does not appear to apply in the smart card/CAM arrangement of Rix. Given these significant differences, one skilled in the art would not be motivated to incorporate the network structure of an online transaction processing scheme into a smart card that has no ability or need to receive communications through a network.

The Examiner on page 7 of the Final Office Action cites MPEP 2144.04(V)(C) as legal precedent as a source of supporting rationale for the motivation to combine Creighton and Rix. MPEP 2144.04(V)(C) states:

> The claimed structure, a lipstick holder with a removable cap, was fully met by the prior art except that in the prior art the cap is "press fitted" and therefore not manually removable. The court held that "if it were considered desirable for any reason to obtain access to the end of the prior art's holder to which the cap is applied, it would be obvious to make the cap removable for that purpose."

Applicants disagree that MPEP 2144.04(V)(C) provides the necessary supporting rationale since the facts in both Rix and Creighton are not sufficiently similar to those in Applicants' application. As noted above, Rix and Creighton involve entirely different environments and address entirely different problems making the facts of these cited references so different that one of ordinary skill in the art would not be motivated to combine them to achieve the claimed invention. Accordingly, one skilled in the art would not look to these references and combine them in the manner suggested.

Applicants submit that for at least the reasons discussed above, the suggested combination of Rix and Creighton fail to disclose, teach, or suggest each and every feature recited in independent claim 1, and thus, claim 1, and the claims that depend therefrom, are believed to be patentably distinguishable over any combination of Rix and Creighton.

The remaining independent claims, claims 10 and 16, and the claims that depend therefrom, recite features similar to those discussed above and are believed to be patentably distinguishable over Rix and Creighton for at least the same reasons as discussed with respect to claim 1. Therefore, withdrawal of the rejection and allowance of Claims 1–2, 4-5, 10–13, and 29–30 is earnestly requested.

B. WHETHER CLAIMS 16–20, 23-27, AND 31 REJECTED UNDER 35 U.S.C. § 103(A) ARE UNPATENTABLE OVER RIX AND FURTHER IN VIEW OF TAKI.

Claims 16-20, 23-27, and 31 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix and further in view of Taki. Applicants respectfully traverse this rejection since Taki is unable to remedy the deficiencies of Rix explained above in conjunction with claim 16, from which the subject claims depend. Accordingly, withdrawal of the rejection is respectfully requested.

C. WHETHER CLAIMS 3 AND 6 REJECTED UNDER 35 U.S.C. § 103(A) ARE UNPATENTABLE OVER RIX, CREIGHTON, AND FURTHER IN VIEW OF OHMORI.

Claims 3 and 6 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Creighton, and further in view of Ohmori. Applicants respectfully traverse this rejection since Ohmori is unable to remedy the deficiencies of Rix and Creighton explained above in conjunction with claim 1, from which the subject claims depend. Accordingly, withdrawal of the rejection is respectfully requested.

D. Whether claims 7-9 and 14-15 rejected under 35 U.S.C. § 103(a) are unpatentable over Rix, Creighton, and further in view of Henrick.

Claims 7-9 and 14-15 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Creighton, and further in view of Henrick. Applicants respectfully traverse this rejection since Henrick is unable to remedy the deficiencies of Rix and Creighton explained above in conjunction with claims 1 and 10, from which the subject claims respectively depend. Accordingly, withdrawal of the rejection is respectfully requested.

E. Whether claims 21 and 28 rejected under 35 U.S.C. § 103(a) are unpatentable over Rix, Taki, and Henrick.

Claims 21 and 28 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Taki, and further in view of Henrick. Applicants respectfully traverse this rejection since Taki and Henrick are unable to remedy the deficiencies of Rix explained above in conjunction with claim 16, from which the subject claims depend. Accordingly, withdrawal of the rejection is respectfully requested.

F. Whether claim 22 is rejected under 35 U.S.C. § 103(a) are unpatentable over Rix, Taki, and further in view of Kuriya.

Claim 22 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Rix, Taki, and further in view of Kuriya. Applicants respectfully traverse this rejection since Taki and Kuriya are unable to remedy the deficiencies of Rix as explained above in conjunction with claim 16, from which the subject claim depends. Accordingly, withdrawal of the rejection is respectfully requested.

G. CONCLUSION

At least the above-identified limitations of the pending claims are not disclosed or suggested by the teachings of the cited references. Accordingly, it is respectfully requested that the Board reverse the rejections of Claims 1–31 under 35 U.S.C. § 103(a).

Please charge the amount of $540.00, covering fee associated with the filing of the Appeal Brief, to **Thomson Licensing Inc., Deposit Account No. 07-0832**. In the event of any non-payment or improper payment of a required fee, the Commissioner is authorized to charge **Deposit Account No. 07-0832** as required to correct the error.

Respectfully submitted,

BY: /Paul P. Kiel/
Paul Kiel, Attorney for Applicants
Registration No.: 40,677
Telephone No.: 609-734-6815

Date: 6/21/11

Thomson Licensing LLC
Patent Operations
P.O. Box 5312
Princeton, NJ 08543-5312

8. CLAIMS APPENDIX

1. (Previously Presented) A device, located at a remote site in communication with a network having at least one server and a content requester, comprising:

a processor in communication with a memory, said processor operable to execute code for:

receiving a first information item comprising an access code and a content key scrambled using a key known by said device, said access code generated by said at least one server in response to a request for a second information item provided by the content requester;

descrambling said first information item using the key known by said device;

transmitting said access code to a server hosting said second information item; and

receiving said second information item scrambled using said content key after said server hosting the second information item verifies said access code.

2. (Original) The device as recited in claim 1, wherein said processor is further operable to execute code for:

descrambling said second information item using said content key.

3. (Original) The device as recited in claim 1, wherein said first information item includes a use-limit indication.

4. (Previously Presented) The device as recited in claim 1, wherein said processor is further operable to execute code for:

transmitting said access code in unencrypted form, said transmitting being selected from the group consisting of : automatically, at a predetermined time, at a predetermined time offset, responsive to a manual input.

5. (Original) The device as recited in claim 1, wherein said content key is selected from the group consisting of: a public key, a shared key.

6. (Original) The device as recited in claim 3, wherein said use-limit indication is selected from the group consisting of : number of uses, time -period.

7. (Original) The device as recited in claim 1, wherein said first information item further includes a content location.

8. (Original) The device as recited in claim 7, wherein said processor is further operable to execute code for transmitting said content location.

9. (Original) The device as recited in claim 7, wherein said content location is known.

10. (Previously Presented) A method, operable at a receiving device located at a remote site in communication with a network having at least one server and a content requester, for descrambling secure content received over said network, said method comprising the steps of:

receiving a first information item comprising an access code and a content key scrambled using a key known by said receiving device, said access code generated by said at least one server in response to a request for a second information item by the content requester;

descrambling said first information item using the key known by said receiving device;

transmitting said access code to a server hosting said second information;

receiving said second information item, scrambled using said content key, after said server hosting the second information item verifies said access code; and

descrambling said second information item using said content key.

11. (Original) The method as recited in claim 10, wherein said first information item includes a use-limit indication.

12. (Original) The method as recited in claim 10, wherein said content key is selected from the group consisting of: a public key, a shared key.

13. (Original) The method as recited in claim 11, wherein said use-limit indication is selected from the group consisting of number of uses, time-period.

14. (Original) The method as recited in claim 10, wherein said first information item further includes a content location.

15. (Original) The method as recited in claim 14, wherein said content location is known.

16. (Previously Presented) A method for transferring secure content over a network comprising the steps of:

receiving a request for content at a first server over a first network from a file requesting device, said request including an encryption key known to a designated remote site;

generating a first information containing an access code and a content key at said first server in response to said request for content by said file requesting device;

transferring said first information item to said designated remote site having a file receiving device, wherein said access code and said content key are scrambled using said encryption key;

receiving said access code from said designated remote site having said file receiving device; and

transferring secure content over a second network after verification of said access code, wherein said secure content is encrypted using said content key.

17. (Original) The method as recited in claim 16, wherein said first network and said second network are the same network.

18. (Original) The method as recited in claim 16, wherein said file requesting device is selected from the group consisting of: personal digital assistant, cellular telephone, notebook computer and personal computer.

19. (Original) The method as recited in claim 16, wherein said file receiving device is selected from the group consisting of: personal digital assistant, cellular telephone, notebook computer and personal computer.

20. (Original) The method as recited in claim 16, wherein said first network is a wireless network.

21. (Original) The method as recited in claim 16, wherein said first information item includes a location of said content.

22. (Original) The method as recited in claim 16, further comprising the step of:

transmitting said content to at least one other server in communication with said first server, wherein said content is scrambled using said content key.

23. (Original) The method as recited in claim 22, further comprising the steps of:

transferring over a second network said secure content after verification of said access code, wherein said secure content is scrambled using said content key.

24. (Original) The method as recited in claim 16, wherein the step of transferring said access code and said content key is over said first network.

25. (Original) The method of as recited in claim 16, wherein the step of transferring said access code and said content key is over said second network.

26. (Original) The method as recited in claim 16, wherein said second network is a high-speed network.

27. (Original) The method as recited in claim 26, wherein said second network is a content delivery network.

28. (Original) The method as recited in claim 16, further comprising the step of:

transferring a location of said content to said remote designated site.

29. (Previously Presented) The device of claim 1, wherein the transmitting step is performed after a predetermined time from when an initial request for said second information item is sent to said at least one server.

30. (Previously Presented) The method of claim 10, wherein the transmitting step is performed after a predetermined delay from when an initial request for said second information item is sent to said at least one server.

31. (Previously Presented) The method of claim 16, wherein the transmitting step is performed after a predetermined delay from when an initial request for said second information item is sent to said at least one server.

9. RELATED EVIDENCE APPENDIX

None.

10. RELATED PROCEEDINGS APPENDIX

None